UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,880	02/27/2002	Nina Lewis	OI7010852003	7239

55498 7590 03/19/2009

ORACLE INTERNATIONAL CORPORATION
c/o VISTA IP LAW GROUP LLP
1885 LUNDY AVENUE
SUITE 108
San Jose, CA 95131

EXAMINER	
GANDHI, DIPAKKUMAR B	
ART UNIT	PAPER NUMBER
2117	

MAIL DATE	DELIVERY MODE
03/19/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/084,880	LEWIS, NINA	
	Examiner	Art Unit	
	DIPAKKUMAR GANDHI	2117	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-24,26-42 and 44-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-24,26-42 and 44-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

1. The amendment filed on 12/08/2008 including amended claims has been entered.

2. Applicant's arguments filed 12/08/2008 have been fully considered but they are not persuasive. The applicant contends that as per claims 1, 19 and 39 the prior arts do not teach the act of determining the local policy for a local scope of access for the user is performed at the local database network node. The examiner disagrees and would like to point out that Moriconi et al. teach that local administrative policy 228 provides a set of policy rules specifying which users are authorized to access management station 212 (fig. 4, col. 9, lines 57-60, Moriconi et al.). Moriconi et al. teach that since the application guards 310 can be distributed among various clients 116, and each application guard 310 has its own specific local client policy 318 (col. 10, lines 18-20, Moriconi et al.).

3. The 35 U.S.C. 101 rejection for claims 19 and 39 is withdrawn.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 1, 54-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) in view of Moriconi et al. (US 6,158,010).

As per claim 1, Cohen et al. teach a method for managing user access information for access to one or more database network nodes, the method comprising: storing database user authentication

information; receiving an access request from the user for the local database network node; authenticating the user based upon the database user authentication information (fig. 2, col. 4, lines 35-45, lines 61-67, col. 5, lines 16-40, Cohen et al.).

However Cohen et al. do not explicitly teach the specific use of storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role, wherein the database user authorization is stored as one or more data objects in the central directory; receiving the user role at a local database network node from the central directory; determining a local policy having user privileges for the local database network node, wherein the local policy is determined by locally processing the user role that is at the central directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated with the central directory, wherein the local policy is different than another local policy determined at another local database network that is on another one of the one or more database network node based on the user role, wherein the act of determining the local policy for a local scope of access for the user is performed at the local database network node; granting the user privileges on the local database network node based upon the local policy; and storing the user privileges in a volatile or non-volatile computer-usable medium.

Moriconi et al. in an analogous art teach a system that combines a centrally managed policy database with distributed authorization (access control) services that enforce the policy for all applications across the organization (col. 3, lines 63-67, Moriconi et al.). Moriconi et al teach that the system comprises a policy manager located on a server…local client policy (col. 4, lines 19-30, Moriconi et al.). Moriconi et al. teach that an authorization…directory servers (col. 6, line 33 - col. 7, line 11, Moriconi et al.). Moriconi et al teach that user of an object…the rule does not evaluate to “false” (col. 7, lines 25 – col. 8, line 31, Moriconi et al.). Moriconi et al. teach that referring now to FIG. 3, a block diagram of one embodiment for non-volatile memory 138, located within client 116 of FIG. 1, is shown. In the FIG. 3 embodiment, non-volatile memory 138 preferably includes an application guard 310 that grants or denies access to various components of client 116, as specified by a pre-determined policy. For example, various components of client 116 can include applications, data, and/or objects. In the FIG. 3 embodiment, application guard

310 preferably includes at least one application 312, an authorization library program 314, an authorization engine program 316, and a local client policy 318 (fig. 3, col. 9, lines 10-20, Moriconi). Moriconi et al. also teach that local administrative policy 228 provides a set of policy rules specifying which users are authorized to access management station 212 (fig. 4, col. 9, lines 57-60, Moriconi et al.). Moriconi et al. teach that since the application guards 310 can be distributed among various clients 116, and each application guard 310 has its own specific local client policy 318 (col. 10, lines 18-20, Moriconi et al.). Moriconi et al. teach that referring now to FIG. 9, a flowchart of one embodiment of menu option navigate tree 814 in management station 212 is shown. Navigate tree 814 provides a set of options for an administrator to add, delete, and/or modify features on server 112 or client 116. The features that an administrator may add, delete, and/or modify include global users 910, global roles 912, directories 914, local roles 916, local users 918, applications 920, application guards 922, and declarations 924. At step 926, the system administrator may then exit from navigate tree 814 (fig. 9, col. 12, lines 31-40, Moriconi et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Moriconi et al. by including an additional step of storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role, wherein the database user authorization is stored as one or more data objects in the central directory; receiving the user role at a local database network node from the central directory; determining a local policy having user privileges for the local database network node, wherein the local policy is determined by locally processing the user role that is at the central directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated with the central directory, wherein the local policy is different than another local policy determined at another local database network that is on another one of the one or more database network node based on the user role, wherein the act of determining the local policy for a local scope of access for the user is performed at the local database network node; granting the user privileges on the local database network node based upon the local policy; and storing the user privileges in a volatile or non-volatile computer-usable medium.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to provide more security in protecting the data using different roles for different users.

- As per claim 54, Cohen et al. and Moriconi et al. teach the additional limitations.

Moriconi et al. teach the method, wherein the one or more privileges are locally defined at the one of the network nodes (col. 3, lines 63-67, col. 4, lines 19-30, Moriconi et al.).

- As per claim 55, Cohen et al. and Moriconi et al. teach the additional limitations.

Moriconi et al. teach the method, wherein the database user authorization is stored in the central directory such that central management of the user role may be performed (col. 6, line 33 - col. 7, line 11, Moriconi et al.).

- As per claim 56, Cohen et al. and Moriconi et al. teach the additional limitations.

Moriconi et al. teach the method, wherein the one or more privileges are not centrally defined at the central directory (col. 3, lines 63-67, col. 4, lines 34-48, Moriconi et al.).

7. Claims 2-4, 11, 12, 13, 14, 15, 16, 17, 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) and Moriconi et al. (US 6,158,010) as applied to claim 1 above, and further in view of Ferguson et al. (US 2002/0082818 A1).

As per claim 2, Cohen et al. and Moriconi et al. substantially teach the claimed invention described in claim 1 (as rejected above).

However Cohen et al. and Moriconi et al. do not explicitly teach the specific use of an LDAP-compatible directory.

Ferguson et al. in an analogous art teach that this is accomplished by user authentication via a lightweight directory access protocol (LDAP) server that authenticates users within particular domain names that map to specific customer accounts (page 4, paragraph 41, Ferguson et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Ferguson et al. by including an additional step of using an LDAP-compatible directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that using an LDAP-compatible directory would provide the opportunity to use a hierarchical structure for user authentication during login process.

- As per claim 3, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which the database user authentication information is stored at the central directory (page 4, paragraph 41, Ferguson et al.).

- As per claim 4, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which the database user authorization is stored in a schema having a hierarchy of schema objects (page 4, paragraph 41, Ferguson et al.).

- As per claim 11, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which the one or more objects are stored in a security subtree in the central directory (figure 1, page 3, paragraph 36, Ferguson et al.).

- As per claim 12, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which administrative access is controlled to one or more data objects in the central directory (page 25, paragraph 196, Ferguson et al.)

- As per claim 13, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which access control is implemented using an access control point associated with the one or more data objects in the central directory (page 19, paragraph 150, Ferguson et al.).

- As per claim 14, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which the access control point is associated with access policies for a subtree of the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 15, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations.

Ferguson et al. teach the method in which the access control point is associated with access policies for a single entry for the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 16, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which the access control point is associated with individually named users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 17, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which the access control point is associated with a group of users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 18, Cohen et al., Moriconi et al., and Ferguson et al. teach the additional limitations. Ferguson et al. teach the method in which members of the group are associated with a set of access privileges associated with the access control point (page 19, paragraph 145, 152, Ferguson et al.).

8. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1), Moriconi et al. (US 6,158,010), and Ferguson et al. (US 2002/0082818 A1) as applied to claim 4 above, and further in view of Gavrila et al. (US 2002/0026592 A1).

As per claim 5, Cohen et al., Moriconi et al., and Ferguson et al. substantially teach the claimed invention described in claim 4 (as rejected above).

However Cohen et al., Moriconi et al., and Ferguson et al. do not explicitly teach the specific use of the method in which the hierarchy of schema objects comprises an enterprise role, wherein the enterprise role is associated with one or more users and one or more locally defined roles.

Gavrila et al. in an analogous art teach that this invention makes use, in yet a further aspect, of both local and global groups for the instantiation of roles on multiple computer hosts, to implement nested groups and to enable the integration of extant host computers, which include local user accounts and groups defined on independent servers and workstations, within large distributed operating systems (abstract, Gavrila et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Gavrila et al by including an additional step of

using the method in which the hierarchy of schema objects comprises an enterprise role, wherein the enterprise role is associated with one or more users and one or more locally defined roles.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to define a global role to associate the users with the authorization to access local databases.

- As per claim 6, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach that the privileges associated with the one or more locally defined roles are assigned to the one or more users (abstract, page 3, paragraph 22, Gavrila et al.).

- As per claim 7, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the method in which the hierarchy of schema objects comprises an enterprise domain, wherein the enterprise domain comprises one or more enterprise roles (page 2, paragraph 10, Gavrila et al.).

- As per claim 8, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the method in which each of the one or more enterprise roles is associated with one or more users and one or more locally defined roles (abstract, Gavrila et al.).

- As per claim 9, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the method in which the enterprise domain is associated with one or more network nodes (page 3, paragraph 22, Gavrila et al.).

9. Claims 19-24, 26-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) in view of Moriconi et al. (US 6,158,010), Ferguson et al. (US 2002/0082818 A1) and Gavrila et al. (US 2002/0026592 A1).

As per claim 19, Cohen et al. teach a system having a processor for managing user access information for one or more database network nodes, comprising: one or more local database network nodes for

which user access is sought; and the user access information data objects comprising authentication (fig. 2, col. 4, lines 35-45, lines 61-67, col. 5, lines 16-40, col. 18, lines 6-8, Cohen et al.).

However Cohen et al. do not explicitly teach the specific use of a LDAP directory; the one or more local database network nodes are associated with the LDAP directory; and user access information data objects stored in the LDAP directory.

Ferguson et al. in an analogous art teach that this database 302 may be accessed by the various agents 304A, 304B, 304C, whose level of access may be determined by a hierarchy of trust component 306. This is accomplished by user authentication via a lightweight directory access protocol (LDAP) server that authenticates users within particular domain names that map to specific customer accounts. The hierarchy of trust component 306 interprets the data related to it from the database 302, and communicates this data, or the interpretation thereof to the various agents 304A, 304B, 304C, and/or the user interface 308 (figure 3, page 4, paragraph 41, Ferguson et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Ferguson et al. by including an additional step of using a LDAP directory; the one or more local database network nodes are associated with the LDAP directory; and user access information data objects stored in the LDAP directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to use a hierarchical structure for user authentication during login process.

Cohen et al. also do not explicitly teach the specific use of the user access information data objects comprising authorization information, wherein the authorization information is associated with a scope of access for a user; one of the collection of roles associated with a privilege that is locally defined at one of the one or more database network nodes; wherein the one or more local database network nodes determines a local policy having the privilege for the user at the local database network node, by defining the scope of access for the user, wherein the privilege is determined by locally processing the one of the collection of roles from the directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated

with the directory, wherein the local policy is different than another local policy determined at another one of the one or more database network node based on the enterprise role.

However Moriconi et al. in an analogous art teach a system that combines a centrally managed policy database with distributed authorization (access control) services that enforce the policy for all applications across the organization (col. 3, lines 63-67, Moriconi et al.). Moriconi et al teach that the system comprises a policy manager located on a server…local client policy (col. 4, lines 19-30, Moriconi et al.). Moriconi et al. teach that an authorization…directory servers (col. 6, line 33 - col. 7, line 11, Moriconi et al.). Moriconi et al teach that user of an object…the rule does not evaluate to "false" (col. 7, lines 25 – col. 8, line 31, Moriconi et al.). Moriconi teaches that referring now to FIG. 3, a block diagram of one embodiment for non-volatile memory 138, located within client 116 of FIG. 1, is shown. In the FIG. 3 embodiment, non-volatile memory 138 preferably includes an application guard 310 that grants or denies access to various components of client 116, as specified by a pre-determined policy. For example, various components of client 116 can include applications, data, and/or objects. In the FIG. 3 embodiment, application guard 310 preferably includes at least one application 312, an authorization library program 314, an authorization engine program 316, and a local client policy 318 (fig. 3, col. 9, lines 10-20, Moriconi). Moriconi et al. also teach that local administrative policy 228 provides a set of policy rules specifying which users are authorized to access management station 212 (fig. 4, col. 9, lines 57-60, Moriconi et al.). Moriconi teaches that since the application guards 310 can be distributed among various clients 116, and each application guard 310 has its own specific local client policy 318 (col. 10, lines 18-20, Moriconi). Moriconi teaches that referring now to FIG. 9, a flowchart of one embodiment of menu option navigate tree 814 in management station 212 is shown. Navigate tree 814 provides a set of options for an administrator to add, delete, and/or modify features on server 112 or client 116. The features that an administrator may add, delete, and/or modify include global users 910, global roles 912, directories 914, local roles 916, local users 918, applications 920, application guards 922, and declarations 924. At step 926, the system administrator may then exit from navigate tree 814 (fig. 9, col. 12, lines 31-40, Moriconi).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Moriconi et al. by including an additional step of using the user access information data objects comprising authorization information, wherein the authorization information is associated with a scope of access for a user; one of the collection of roles associated with a privilege that is locally defined at one of the one or more database network nodes; wherein the one or more local database network nodes determines a local policy having the privilege for the user at the local database network node, by defining the scope of access for the user, wherein the privilege is determined by locally processing the one of the collection of roles from the directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated with the directory, wherein the local policy is different than another local policy determined at another one of the one or more database network node based on the enterprise role.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to provide more security in protecting the data using scope of access for different users.

Cohen et al. also do not explicitly teach specifically that the user access information data objects are associated with an enterprise role, the enterprise role comprising a collection of roles.

However Gavrila et al. in an analogous art teach local and global groups for the instantiation of roles on multiple computer hosts (abstract, Gavrila et al.). Gavrila et al. also teach role instances of a role on a host computer or set of host computers…both instances were derived on the same set of host computers (page 3, paragraph 22, Gavrila et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Gavrila et al. by including an additional step of using the user access information data objects associated with an enterprise role, the enterprise role comprising a collection of roles.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide

the opportunity to define a global role to associate the users with the authorization to access local databases.

- As per claim 20, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the user access information data objects comprise a domain object that is associated with the one or more database network nodes (page 8, paragraph 98-99, Gavrila et al.).

- As per claim 21, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the domain object is associated with the enterprise role (page 8, paragraph 99, Gavrila et al.).

- As per claim 22, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the enterprise role is associated with a local database role (abstract, page 3, paragraph 22, Gavrila et al.).

- As per claim 23, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the scope of the local database role is locally defined at a local database network node (page 3, paragraph 22, Gavrila et al.).

Ferguson et al. teach database (page 4, paragraph 41, Ferguson et al.).

- As per claim 24, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the enterprise role is associated with another user (page 3, paragraph 22, Gavrila et al.).

- As per claim 26, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the user access information data objects comprise an access control point attribute (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 27, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is established only if access control policies are established for a corresponding object (page 19, paragraph 145, Ferguson et al.).

- As per claim 28, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with access policies for a subtree in the user access information data objects stored in the LDAP directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 29, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with access policies for a single entry in the user access information data objects stored in the LDAP directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 30, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with individually named users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 31, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the access control point attribute is associated with a group of users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 32, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which members of the group are associated with a set of access privileges associated with the access control (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 33, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the user access information data objects comprise a mapping object that maps a database user to a database schema (page 4, paragraph 41, Ferguson et al.).

- As per claim 34, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object affects a single user (page 4, paragraph 41, Ferguson et al.).

- As per claim 35, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object is associated with a full distinguished name (page 4, paragraph 41, Ferguson et al.).

- As per claim 36, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object is associated with a plurality of users (page 4, paragraph 41, Ferguson et al.).

- As per claim 37, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Ferguson et al. teach the system in which the mapping object is associated with a partial distinguished name (page 4, paragraph 41, Ferguson et al.).

- As per claim 38, Cohen et al., Moriconi et al., Ferguson et al. and Gavrila et al. teach the additional limitations.

Gavrila et al. teach the system in which the enterprise role is associated with local database roles from a plurality of database nodes (abstract, Gavrila et al.).

10. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) in view of Moriconi et al. (US 6,158,010) and Gavrila et al. (US 2002/0026592 A1).

As per claim 39, Cohen et al. teach a process for managing user access information for database network nodes, the process comprising: storing database user authentication information; receiving an access request from a user for the local database network node; authenticating the user based upon the database user authentication information (fig. 2, col. 4, lines 35-45, lines 61-67, col. 5, lines 16-40, Cohen et al.).

However Cohen et al. do not explicitly teach the specific use of storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role, wherein the database user authorization is stored as one or more data objects in the central directory; receiving the user role at a local database network node from the central directory; determining a local policy having user privileges for the local database network node, wherein the local policy is determined by locally processing the user role that is at the central directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated with the central directory; wherein the local policy is different than another local policy determined at another local database network node that is on another one of the one or more database network node and the another local policy is based on the user role, wherein the act of determining the local policy for a local scope of access for the user is performed at the local database network node; and granting the user privileges on the local database network node based upon the local policy.

Moriconi et al. in an analogous art teach a system that combines a centrally managed policy database with distributed authorization (access control) services that enforce the policy for all applications across the organization (col. 3, lines 63-67, Moriconi et al.). Moriconi et al teach that the system comprises a policy manager located on a server…local client policy (col. 4, lines 19-30, Moriconi et al.). Moriconi et al. teach that an authorization…directory servers (col. 6, line 33 - col. 7, line 11, Moriconi et al.). Moriconi et al teach that user of an object…the rule does not evaluate to “false” (col. 7, lines 25 – col. 8, line 31, Moriconi et al.). Moriconi teaches that referring now to FIG. 3, a block diagram of one embodiment for

non-volatile memory 138, located within client 116 of FIG. 1, is shown. In the FIG. 3 embodiment, non-volatile memory 138 preferably includes an application guard 310 that grants or denies access to various components of client 116, as specified by a pre-determined policy. For example, various components of client 116 can include applications, data, and/or objects. In the FIG. 3 embodiment, application guard 310 preferably includes at least one application 312, an authorization library program 314, an authorization engine program 316, and a local client policy 318 (fig. 3, col. 9, lines 10-20, Moriconi). Moriconi et al. also teach that local administrative policy 228 provides a set of policy rules specifying which users are authorized to access management station 212 (fig. 4, col. 9, lines 57-60, Moriconi et al.). Moriconi teaches that since the application guards 310 can be distributed among various clients 116, and each application guard 310 has its own specific local client policy 318 (col. 10, lines 18-20, Moriconi). Moriconi teaches that referring now to FIG. 9, a flowchart of one embodiment of menu option navigate tree 814 in management station 212 is shown. Navigate tree 814 provides a set of options for an administrator to add, delete, and/or modify features on server 112 or client 116. The features that an administrator may add, delete, and/or modify include global users 910, global roles 912, directories 914, local roles 916, local users 918, applications 920, application guards 922, and declarations 924. At step 926, the system administrator may then exit from navigate tree 814 (fig. 9, col. 12, lines 31-40, Moriconi). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Moriconi et al. by including an additional step of storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role, wherein the database user authorization is stored as one or more data objects in the central directory; receiving the user role at a local database network node from the central directory; determining a local policy having user privileges for the local database network node, wherein the local policy is determined by locally processing the user role that is at the central directory, wherein the act of locally processing is performed at the local database network node that is one of the one or more database network nodes that is associated with the central directory; wherein the local policy is different than another local policy determined at another local database network node that is on another one of the one or more database network node and the another local

policy is based on the user role, wherein the act of determining the local policy for a local scope of access for the user is performed at the local database network node; and granting the user privileges on the local database network node based upon the local policy.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to provide more security in protecting the data using different roles for different users.

Cohen et al. also do not explicitly teach the specific use of a computer program product that includes a volatile or non-volatile computer-usable medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process.

However Gavrila et al. in an analogous art teach a computer program product containing computer readable code for causing a machine to perform the method (page 19, claim 22, Gavrila et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Gavrila et al. by including an additional step of using a computer program product that includes a volatile or non-volatile computer-usable medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that using a computer program product that includes a medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process would provide the opportunity to execute the process automated, faster and accurately.

11. Claims 40-42, 44-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1), Moriconi et al. (US 6,158,010) and Gavrila et al. (US 2002/0026592 A1) as applied to claim 39 above, and further in view of Ferguson et al. (US 2002/0082818 A1).

As per claim 40, Cohen et al., Moriconi et al. and Gavrila et al. substantially teach the claimed invention described in claim 39 (as rejected above).

However Cohen et al., Moriconi et al. and Gavrila et al. do not explicitly teach the specific use of the central directory comprising an LDAP-compatible directory.

Ferguson et al. in an analogous art teach that this is accomplished by user authentication via a lightweight directory access protocol (LDAP) server that authenticates users within particular domain names that map to specific customer accounts (page 4, paragraph 41, Ferguson et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Ferguson et al. by including an additional step of using the central directory comprising an LDAP-compatible directory.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that using the central directory comprising an LDAP-compatible directory would provide the opportunity to use a hierarchical structure for user authentication during login process.

- As per claim 41, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the database user authentication information is stored at the central directory (page 4, paragraph 41, Ferguson et al.).

- As per claim 42, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the database user authorization is stored in a schema having a hierarchy of schema objects (page 4, paragraph 41, Ferguson et al.).

- As per claim 44, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the one or more objects are stored in a security subtree in the central directory (figure 1, page 3, paragraph 36, Ferguson et al.).

- As per claim 45, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that administrative access is controlled to one or more data objects in the central directory (page 25, paragraph 196, Ferguson et al.).

- As per claim 46, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that access control is implemented using an access control point associated with the one or more data objects in the central directory (page 19, paragraph 150, Ferguson et al.).

- As per claim 47, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with access policies for a subtree of the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 48, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with access policies for a single entry for the one or more database objects in the central directory (page 19, paragraph 145, Ferguson et al.).

- As per claim 49, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with individually named users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 50, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that the access control point is associated with a group of users (page 18-19, paragraph 144-145, Ferguson et al.).

- As per claim 51, Cohen et al., Moriconi et al., Gavrila et al. and Ferguson et al. teach the additional limitations.

Ferguson et al. teach that members of the group are associated with a set of access privileges associated with the access control point (page 19, paragraph 145, 152, Ferguson et al.).

12. Claims 52, 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 6,178,511 B1) and Moriconi et al. (US 6,158,010) as applied to claim 1 above, and further in view of Franklin et al. (US 2001/0023440 A1).

As per claim 52, Cohen et al. and Moriconi et al. substantially teach the claimed invention described in claim 1 (as rejected above).

However Cohen et al. and Moriconi et al. do not explicitly teach the specific use of the method, wherein one of the one or more data objects comprises a distinguished name, wherein the distinguished name comprises a common name having a value for identifying a database.

Franklin et al. in an analogous art teach that a user object 98 is associated with an individual user. The distinguished name 144 of FIG. 6 is exemplary of all distinguished names 124. Each distinguished name 124 typically includes a common name 146 in association with a context 148. Context 148 may include acronyms, abbreviations, or other identifications of organizations, geography, logical relationships, and enterprises, as illustrated (fig. 5, 6, page 4, paragraph 53, Franklin et al.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Cohen et al.'s patent with the teachings of Franklin et al. by including the method, wherein one of the one or more data objects comprises a distinguished name, wherein the distinguished name comprises a common name having a value for identifying a database.

This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that it would provide the opportunity to identify a database.

- As per claim 53, Cohen et al., Moriconi et al. and Franklin et al. teach the additional limitations.

Franklin et al. teach the method, wherein one of the one or more data objects comprises a distinguished name, wherein the distinguished name comprises a common name having a value for representing an administrative context, a root context, or a user-fined context (fig. 5, 6, page 4, paragraph 53, Franklin et al.).

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DIPAKKUMAR GANDHI whose telephone number is (571)272-3822. The examiner can normally be reached on 9:00 AM - 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Cynthia Britt/
Primary Examiner, Art Unit 2117

/Dipakkumar Gandhi/
Examiner, Art Unit 2117